What is claimed is:

1. A tamper-resistant computer system having a CPU and a main memory for executing application software, comprising:

a first operating system; and

a second operating system;

wherein the application software comprises a first component program executed by the first operating system, and a second component program executed by the second operating system, wherein the first component program has a user interface for receiving an operational instruction from a user of the computer system and for issuing a command to the second component program, and

wherein the second component program performs the command issued by the first component program if execution thereof has been designated as permitted in advance, thereby preventing the second component program from being accessed by the user.

2. A tamper-resistant computer system as claimed in claim 1, further comprising a communication control program that sends a command issued by the first component program to the second component program if execution thereof is permitted.

3. A tamper-resistant computer system as claimed in claim 2, further comprising a multi-OS control program for controlling the first and second operating systems;

wherein the multi-OS control program establishes a particular region in a memory area managed by the first operating system so that the particular region can be referred to by the communication control program, wherein the user interface of the first component program writes the command into the particular region for issuance thereof, and

wherein, by referring to the particular region, the communication control program reads a command stored in the particular region by the first component program, and then, by making reference to a list of the permitted commands held in a memory area managed by the second operating system, the communication control program sends the command to the second component program if the command is in the list.

4. A tamper-resistant computer system as claimed in claim 3 further including a tamper-resistant hardware module for storing a system boot program;

wherein the tamper-resistant computer system includes an initial program for reading the system boot program at system startup,

wherein the system boot program includes a function for executing the multi-OS control program, and wherein the multi-OS control program includes a function for executing the first and second operating systems.

5. A tamper-resistant computer system as claimed in claim 4,

wherein the second component program comprises a system boot program, cryptographic software, and digital signature, wherein the hardware module includes a decryption key for the cryptographic software and a function for authenticating the system boot program,

wherein the system boot program includes a function for performing authentication for the hardware module, a function for extracting the decryption key for the cryptographic software from the hardware module, and a function for decrypting the cryptographic software with the decryption key extracted from the hardware module, and

wherein, according to a command from the first component program, the system boot program is executed, and in response the cryptographic software is decrypted and executed.

6. A tamper-resistant computer system as claimed in claim 5 wherein the hardware module further includes a decryption key for cryptographic data to be used by the second component program, and wherein the second component decrypts the cryptographic data.

7. A tamper-resistant computer system as claimed in claim 3,

wherein, at start of the second component program, the second component program adds a command permitted for the first component program to the list of permitted commands, and

wherein, at the time of termination of the second component program, the second component program removes the command from the list of permitted commands.

8. A tamper-resistant computer system as claimed in claim 1, wherein the second component program comprises a command processing program for command execution, and a communication control program through which a command issued by the

first component program is sent to the command processing program if execution thereof is permitted.

9. A method for installing system software onto a tamper-resistant computer system comprising:

providing an installation program for system software which includes an installation start program, a cryptographic system file, and a digital signature, and wherein the installation start program includes a function for extracting a decryption key for the cryptographic system file from the hardware module and a function for decrypting the cryptographic system file with the decryption key extracted from the hardware module; and

executing the installation start program; and decrypting the cryptographic system file.

10. A method as in claim 9, wherein the method further comprises:

providing an installation program for application software which installation program includes a first installation program executed by a first operating system and a second installation program executed by a second operating system; wherein the first installation program includes a function for writing a first component program into a memory area managed by the first operating system and a function for calling the second installation program, wherein the second installation program has a function for writing the second component program into a memory area managed by the second operating system;

executing the first installation program;

calling the second installation program; and

executing the second installation program.

11. A method as in claim 9, wherein the installation program for the application software includes a digital signature, and a step is performed of checking the digital signature before writing the first and second component programs into the memory areas.